CLAIMS

What is claimed:

1. A server mediated security token access method comprising the steps of:

   a. exchanging one or more critical security parameters between a security token enabled client, a security token operatively coupled to said security token enabled client and an authentication server, wherein said security token is generally unavailable to a user due to implementation of a security policy or a processing limitation,

   b. performing a plurality of authentication transactions between at least said security token and said authentication server using said one or more critical security parameters, and

   c. allowing said user access to one or more security token resources following successful completion of said plurality of authentication transactions.

2. The method according to claim 1 wherein step 1.a further includes the steps of;

   a. generating by either said security token or said security token enabled client, an access request which incorporates a unique identifier associated with said security token,

   b. sending said access request to said authentication server, and

   c. obtaining a critical security parameter associated with said unique identifier, wherein said critical security parameter is a member of said one or more critical security parameters.

3. The method according to claim 1 wherein said one or more critical security parameters is selected from the group consisting of a passphrase, a cryptographic key, biometric data, a password, a security state associated with said security policy and a result of a cryptographic operation.

4. The method according to claim 1 further including the step of establishing a secure messaging session between said authentication server and at least said security token.

5. The method according to claim 1 further including the step of resetting an invalid entry counter associated with said security token following successful completion of said plurality of authentication transactions.

6. The method according to claim 4 wherein said secure messaging session incorporates a set of session keys generated by said authentication server and shared with said security token.

7. The method according to claim 4 wherein said secure messaging session incorporates an APDU communications pipe.

8. The method according to claim 4 wherein said secure messaging session includes SSL, IPsec or TLS.

9. The method according to claim 3 wherein said biometric data is sent from said security token enabled client to said authentication server, processed by said authentication server and returned to said security token as a member of said one or more critical security parameters.

10. The method according to claim 3 wherein said biometric data is sent from said security token enabled client to said authentication server, processed by said authentication server, matched against a reference biometric template and a cryptographic result returned to said security token as a member of said one or more critical security parameters.

11. A server mediated security token access system comprising:

a security token enabled client in processing communications with an authentication server and an operatively coupled security token, wherein said security token enabled client includes means for;

- receiving a first critical security parameter from a user,
- exchanging a plurality of critical security parameters between said security token and said authentication server, wherein said first critical security parameter is a member of said plurality of critical security parameters,
- generating an access request which incorporates a unique identifier associated with said security token,
- sending an access request and at least one member of said plurality of critical security parameters to said authentication server, and

said authentication server including means for;

- authenticating said user via at least said at least one member,
- obtaining a second critical security parameter having an association with said security token, wherein said second critical security parameter is also a member of said plurality of critical security parameters, and
- sending said second critical security parameter to said security token;

said security token including means for;

- authenticating said second critical security parameter, and
- allowing access to one or more security token resources following successful authentication of said second critical security parameter.

12. The system according to claim 11 wherein said authentication server further includes means for generating and sharing a set of session keys with said security token.

13. The system according to claim 11 wherein said processing communications includes SSL, IPsec or TLS.

14. The system according to claim 12 wherein said authentication server and said security token further includes means for establishing a secure messaging session between said authentication server and said security token using said set of session keys.

15. The system according to claim 12 wherein said security token further includes means for generating and assigning session identifiers to said set of session keys.

16. The system according to claim 11 wherein said plurality of critical security parameters is selected from the group consisting of a passphrase, a cryptographic key, biometric data, a password, a security state associated with a security policy and a result of a cryptographic operation.

17. The system according to claim 11 wherein said authentication server further includes means for;

- processing a biometric sample sent from said security token enabled client as said first critical security parameter,
- generating a sample biometric template,
- matching said sample biometric template against a reference biometric template and returning a cryptographic result to said security token as said second critical security parameter, or
- sending said sample biometric template to said security token as said second critical security parameter.

18. The system according to claim 11 wherein said authentication server further includes means for resetting an invalid entry counter associated with said security token following authentication of said second critical security parameter.

19. The system according to claim 11 wherein said security token is generally unavailable to said user due to implementation of a security policy or a processing limitation.

20. The system according to claim 16 wherein said security policy is associated with at least said security token, said security token enabled computer system or said authentication server.

21. A server mediated security token access system comprising:

a security token enabled client in processing communications with an authentication server and an operatively coupled security token including;

a user input means;

a first processor;

a first memory operatively coupled to said first processor;

a client application operatively stored in at least a portion of said first memory having logical instructions executable by said first processor to;

receive a first critical security parameter from said user input means,

exchange a plurality of critical security parameters between said security token and said authentication server, wherein said first critical security parameter is a member of said plurality of critical security parameters,

generate an access request which incorporates a unique identifier associated with said security token, and

send said access request to said authentication server;

said authentication server including;

a second processor;

a second memory operatively coupled to said second processor;

a server application operatively stored in at least a portion of said second memory having logical instructions executable by said second processor to;

authenticate a user via said first critical security parameter,

obtain a second critical security parameter associated with said security token via said unique identifier, wherein said second critical security parameter is also a member of said plurality of critical security parameters, and

send said second critical security parameter to said security token; and

said security token including;

a third processor;

a third memory operatively coupled to said third processor;

a security executive application operatively stored in at least a portion of said third memory having logical instructions executable by said third processor to;

authenticate said second critical security parameter, and

allow access to one or more security token resources following successful authentication of said second critical security parameter;

wherein said security token is generally unavailable to said user due to implementation of a security policy or a processing limitation.

22. The system according to claim 21 wherein said authentication server further includes a pipe server application operatively installed in another portion of said second memory having logical instructions executable by said second processor to;

generate APDU commands,

encapsulate said APDU commands in one or more communications packets, and

extract APDU responses encapsulated in said one or communications packets.

23. The system according to claim 22 wherein said security token enabled client further includes a pipe client application operatively installed in another portion of said first memory having logical instructions executable by said first processor to;

encapsulate said APDU responses in one or more communications packets, and

extract said APDU commands encapsulated in said one or communications packets.

24. The system according to claims 21 wherein said plurality of critical security parameters is selected from the group consisting of a passphrase, a cryptographic key, biometric data, a password, a security state associated with a security policy and a result of a cryptographic operation.

25. The system according to claim 21 wherein said client application further includes logical instructions executable by said first processor to receive a biometric sample from said user and send said biometric sample to said authentication server as said first critical security parameter.

26. The system according to claim 21 wherein said server application authentication further includes logical instructions executable by said second processor to;

- process a biometric sample sent from said security token enabled client as said first critical security parameter,
- generate a sample biometric template,
- match said sample biometric template against a reference biometric template and return a cryptographic result to said security token as said second critical security parameter, or
- send said sample biometric template to said security token as said second critical security parameter.

27. The system according to claim 21 wherein said processing communications includes SSL, IPsec or TLS.

28. The system according to claim 21 wherein said processing communications includes a set of session keys generated by said authentication server and shared with said security token.

29. A computer program product embodied in a tangible form readable by a plurality of processors in processing communications, wherein said computer

program product includes executable instructions stored thereon for causing one or more of said plurality of processors to;

a. exchange a plurality of critical security parameters between a first processor, a second processor and a third processor,

b. authenticate a first member of said plurality of critical security parameters received by said second processor,

c. send a second member of said plurality of critical security parameters to said third processor following authentication of said first member of said plurality of critical security parameters by said second processor,

d. authenticate said second member of said plurality of critical security parameters by said third processor, and

e. allow access to a memory coupled to said third processor following successful authentication of said second member of said plurality of critical security parameters.

30. The computer program product according to claim 28 wherein said tangible form includes magnetic media, optical media or logical media.

31. The computer program product according to claim 28 wherein said executable instructions are stored in a code format selected from the group consisting of compiled, interpreted, compilable and interpretable.